Guidance for Safety Aspects of Proposed Hydrogen Projects

July 2003
Revision 1

U.S. Department of Energy
Hydrogen, Fuel Cells & Infrastructure Technologies Program

Table of Contents

Guidance for Safety Aspects of Proposed Hydrogen Projects

Overview

This guidance document provides proposers with clarification on safety requirements for hydrogen-related solicitations from the U.S. Department of Energy Hydrogen, Fuel Cells and Infrastructure Technologies Program. **All proposals for hydrogen-related solicitations must include a preliminary safety plan, and all funded projects must complete a more detailed safety plan as part of the project.**

The document will explain the objectives that must be met and provide examples, but it will not outline the detailed steps that must be completed in a safety plan. The responsibility of selecting the specific safety methodology and the justification of that method falls upon the principal investigator and collaborating research groups. Standard practices exist for the qualification of safety hazards, and the proposers must choose which are best for their project.

Safe practices in the production, storage, distribution, and use of hydrogen are essential for insurability and for the widespread acceptance of hydrogen technologies. A catastrophic failure in any hydrogen project could damage the insurance industry's, as well as the public's perception of hydrogen and fuel cells. The Hydrogen, Fuel Cells and Infrastructure Technologies Program is developing and implementing practices that, if implemented early in a project, will provide an environment *where safety is an integral component of any Department of Energy-funded project*.

A safety plan identifies immediate (primary) failure modes as well as any secondary failure modes that may come about as a result of other failures. In such a plan, every conceivable failure is identified, from catastrophic failures to benign collateral failures. The documentation of benign failures can be used to address a more serious failure.

All potential hazards in a hydrogen production, delivery, utilization, or storage system must be identified and analyzed, as well as any system aspects that may be adversely affected by a failure. These aspects include:

- **Personnel.** The identification and mitigation of any hazards that pose a risk of injury or loss of life to personnel. A complete safety assessment considers not only those personnel who are directly involved in a hydrogen process, but also those who may not be involved in the process at all, but are still at risk due to these hazards.
- **Equipment.** The prevention of damage to or loss of equipment. Damage to equipment can be both the cause of incidents and the result of incidents. An equipment failure can result in collateral damage to nearby equipment, which can trigger additional equipment failures or even present additional risks to personnel. A complete safety plan must consider and minimize any risk of equipment damage.
- **Environment.** Any damage to the environment. Any aspect of a natural or built environment that can be harmed due to a failure is identified and analyzed. A qualification of the failure modes resulting in environmental damage must be included in the safety plan.

Project proposals should include a preliminary safety plan that identifies safety hazards. Systematic procedures must be used to consider design modifications and alternatives to reduce risks when hazards are identified, and should include mitigation (passive and active ventilation, for example) in the case of unforeseen circumstances.

Based on the type of proposal to be submitted, the following items must be addressed. Proposals relating to computational or analytical work, in which no experiments are to be performed, do not require a safety plan.

A) Hydrogen Technology Validation and Demonstration Projects

The following items must be included in the preliminary safety plan for the proposal:

1. **Identification of Safety Vulnerabilities (ISV)** – one out of 3 options shall be used: (1) Preliminary Failure Modes and Effects Analysis (FMEA), (2) hazard analysis, or (3) probability risk assessment**.** In addition to the preliminary ISV evaluation, a plan for preparing the final analysis or assessment that identifies significant safety concerns should be included. This final analysis will be due within 90 days after the contract is awarded. Published data should be used when available. If data are not available, engineering practice may be used. The approach should be explained if it differs from industry practice.
2. **Brief example of a safety assessment** (up to 3 pages) for installing a new system or testing a new piece of equipment, including calculations.
3. **Detailed outline of the Risk Mitigation Plan** that will apply to the project based on the preliminary FMEA/analysis/assessment.
4. **Description of how safety performance will be measured and monitored** to ensure that the FMEA/analysis/assessment is updated regularly as data becomes available.
5. **Detailed outline for the Communications Plan** that the project manager will develop and implement during the project. This should include a description of reportable accidents, management response, and independent reviews during the design/development and operations phases of the project and how they will be reported.

The preliminary safety plan should be submitted as an Attachment to the proposal through the Industry Interactive Procurement System (IIPS) submission process at http://e-center.doe.gov.

B) Research and Development Projects

A safety plan will not be required until after contracts are awarded. However, R&D proposals involving the use of hydrogen should briefly describe the process to be used for evaluating, reviewing, and implementing a safety plan as part of the proposed R&D work (up to 1 page maximum). This process description should clearly indicate participation of all collaborating research groups and appropriate personnel (safety engineers, researchers, students, postdocs, etc). The safety process definition may either be submitted as part of the proposal (e.g. within the Management Plan) or may be submitted as an Attachment through the Industry Interactive Procurement System (IIPS) submission process at http://e-center.doe.gov. Individual solicitations may provide further direction on where to address safety planning within the proposal. Note that safety planning must be addressed in full-proposals: pre-applications do not require safety planning descriptions.

A safety plan will be required within 90 days after the contract is awarded. The following items must be included in the safety plan:

1. **Identification of Safety Vulnerabilities (ISV)** An assessment of potential safety concerns. Examples of options that may be used are: (1) Preliminary Failure Modes and Effects Analysis (FMEA), (2) hazard analysis, or (3) probability risk assessment**.**
2. **Brief example of a safety assessment** (up to 1 page) if applicable, for installing a new system or testing a new piece of equipment, including calculations such as concentrations of hydrogen to be produced or tested.
3. **Outline of the Risk Mitigation Plan** that will apply to the project based on the FMEA/analysis/assessment.
4. **Description of how safety performance will be measured and monitored** to ensure that the FMEA/analysis/assessment is updated regularly as data becomes available.
5. **Detailed outline for the Communications Plan** that the project manager will develop and implement during the project. This should include a description of reportable accidents, management response, and independent reviews during the design/development and operations phases of the project and how they will be reported.

General guidance and examples for preparing a safety plan are covered below. Additional examples may be provided once contracts have been awarded.

Identification of Safety Vulnerabilities

The preliminary Identification of Safety Vulnerabilities (ISV) can take the form of a Preliminary Failure Modes and Effects Analysis (FMEA), hazard analysis, or probability risk assessment**,** and demonstrates that the proposer has assessed safety early in the process and has integrated it into the proposed project. The three methodologies are all established industry standards for reliability engineering. The purpose is to analyze design components for safety hazards and to demonstrate an understanding and anticipation of component failures. The most important objective is the prevention of problems before they occur. In the case of a failure, the ISV will minimize the effects of that failure. In a sense, it is a reliability tool as well as a safety tool, as it can help to identify areas within a system that are prone to failure.

Prior to performing the ISV, efforts should be made to compile information central to the system. Pertinent information includes:

- component specifications and configurations,
- component interaction information,
- operating procedures, and
- equipment types.

Information from earlier projects may be effective in the collection of the above information.

An example of a hazard identification table is shown in Appendix A.

FMEA

Various methodologies exist for the creation of a FMEA, and numerous FMEA guides are available from traditional industry sources. Guidelines on general safety information are available in various government and military documents, including MIL-STD-882C and MIL-STD-1629A. In addition, websites such as **http://www.fmeainfocentre.com/** (a non-commercial web-based inventory dedicated to the promotion of Failure Mode and Effect Analysis) and the NASA Technical and Information Program's **http://www.sti.nasa.gov/new/fmea33.html** may provide additional information on the development of FMEAs.

In general, the FMEA process follows a standard procedure, as detailed below:

1. Identify top level hazards/events
2. Identify related equipment/components/processes
3. Identify potential failures
4. Identify design safety
5. Identify corrective actions

This outline is repeated for every hazard or component for a complete system.

A FMEA can be preformed via two different approaches. The hardware, or component, analysis is the identification and analysis of ramifications of component failures. This method is a bottom-up approach, wherein failures are initiated on the subsystem level. The functional approach is a top-down method, more suitable when specific components have not yet been chosen. Either approach is acceptable. The development of the FMEA is a continuous process, and the document should evolve as the system design changes.

A sample excerpt from a FMEA table is shown in Appendix B.

Safety Assessment

Each project's proposal will be evaluated for its thorough investigation and reporting of safety hazards. Therefore, a brief example of a safety assessment (up to 3 pages) for installing a new system or testing a new piece of equipment, including calculations, is required. Below is an approach for a safety assessment.

1. Perform safety assessment before construction begins—during design phase. Maintain construction oversight throughout the project.
2. Review system design against existing codes and standards (ASME, NFPA, etc.)
3. Develop detailed, reasonable-worst-case, credible scenarios describing process upsets, human errors, system failures, etc. that could result in unwanted or unacceptable consequences. These scenarios can be postulated without regard to existing design safety features.
4. Identify and correct construction and code problems and deviations
    a. Identify and brief appropriate permit, regulatory, and safety personnel early in the project (site/location specific)
    b. Address mechanical and/or electrical issues, storage separation distances, component ratings, etc.
    c. Identify "new" hazards, if any—some hazards are equivalent to other commonly accepted public and industrial hazards
    d. Hazards can be characterized in terms of form, quantity, and location.

Detailed Outline of Risk Mitigation Plan

The purpose of a risk mitigation plan is to outline and minimize the risks that hold the greatest potential for harm. It is essentially an extension of the ISV, as its construction usually follows that development. After identifying safety vulnerabilities, the proposer will have a prioritized list of safety aspects that require action. A risk mitigation plan provides detailed design and operational modifications for each issue on that list. Typical aspects of a risk mitigation plan include a discussion of mitigation measures, a cost-benefit analysis, and an implementation strategy.

A detailed outline of the risk mitigation plan would assess the scenarios and identified hazards from the safety assessment. The plan should determine the likelihood of occurrence, which could be expressed in frequency of occurrence, and the severity of consequence. It should consider the cause(s) of the scenario (or initiating event[s]) and the hazardous material or energy released as a

result of the scenario. During this phase of the analysis, no credit is taken for preventive or mitigative features in reducing frequency or consequence, thereby focusing on those hazards that are of greatest concern.

The following categories could be used for organizing and analyzing data:

- Event number
- Event category
- Postulated event description
- Causes
- Preventive features
- Frequency level
- Mitigative features
- Consequences
- Risk bin number

Risk binning is one analysis tool for risk mitigation. Each hazard can be plotted on a frequency/consequence matrix, which would indicate its level of risk – high, moderate, low, or negligible. For example, if a potential hazard's frequency is unlikely, and its consequence level is high, it would be a high risk.

An example of a risk-binning matrix and frequency and consequence criteria tables are shown in Appendix C.

Safety Performance Measurement and Monitoring

A good measure of a safe hydrogen project is its insurability, and an important step is to quantify risks. A thorough safety plan will serve as a basis on which the risks associated with a technology may be measured. Each project proposal needs to include a description of how safety performance will be measure and monitored, to ensure that the FMEA is updated regularly as data becomes available.

Communications Plan Outline

The communications plan is an outline of reports that are made when an incident occurs. A reportable incident is broadly defined as a failure that results in damage to any of the factors (personnel, equipment, environment) discussed above. The magnitude of these risks can vary widely, and some discretion is left to the investigator. However, certain incidents are reportable under any conditions. These failures are as follows:

- Any failure that results in a modification to any part of the FMEA
- Any failure that results in a injury or lost time accident
- Any failure that results in down time to process equipment

This list is not inclusive of all reportable incidents, but is indicative of the severity of incidents that must be reported.

Appendix A

Example Hazard Identification Table

Table 1-1.–HAZARD ENERGY SOURCES, MATERIALS AND EQUIPMENT

Location (identifier for system, sub-system, or operational feature in this facility section)	Hazard Energy Sources and Materials: Electrical: Battery Banks (BB)	Cable Runs (CB)	Diesel Units (DU)	Electrical Equipment (EE)	Hot Plates (HP)	Heaters (HT)	High Voltage (HV,>220 v)	Locomotive, Electrical (LE)	Motors (MT)	Pumps (PM)	Power Tools (PT)	Switchgear (SG)	Service Outlets, fittings (SO)	Transformers (TF)	Transmission Lines (TL)	Underground Wiring (UW)	Wiring (WR)	Other	Thermal: Bunsen Burner, Hot Plates (BR)	Electrical Equipment (EE)	Furnaces (FR)	Heaters (HT)	Steam Lines (SL)	Welding Torch (WT)	Exothermic Reactions (ER)	Other	Friction: Belts (BL)	Bearings (BR)	Fans (FN)	Gears (GE)	Motors (MT)	Power Tools (PT)	Other
Working vehicle	X	-	-	X	X	-	1	X	X	X	X	-	X	X	2	-	X	3	-	X	-	-	-	X	4	5	X	X	X	X	X	X	X
Underground refueling operation	X	-	-	X	X	-	1	X	X	X	X	-	X	X	2	-	X	3	-	X	-	-	-	X	X	5	X	X	X	X	X	X	X
Refueling transport vehicle	X	-	-	X	X	-	1	X	X	X	X	-	X	X	2	-	X	3	-	X	-	-	-	X	4	5	X	X	X	X	X	X	X
Fuel transfer (not covered)																																	
Hydrogen mfg. (not covered)																																	

Location (identifier for system, sub-system, or operational feature in this facility section)	Hazard Energy Sources and Materials: Pyrophoric (Pu & U Metal (PU)	Pyrophoric (Other)	SC (Nitric Acid and Organics) (HN)	SC (Other)	Combustible Materials (CB)	Uncontrolled Chem. Reactions (CH)	Open Flame: Bunsen Burners (BR)	Torches (WT)	Pilot Lights (PL)	Gas Welding (GW)	Other	Flammables: Flammable Gases (FG)	Flammable Liquids (FL)	Flammable Mixtures (FA)	Other	Explosives: Explosive Gases (EG)	Hydrogen/Tritium (HZ)	Propane (PP)	Explosive Chemicals (EC)	Other	Potential: Gas Bottles (GB)	Gas Receivers (GR)	Pressure Vessels (PV)	Steam Headers/Lines (ST)	Other	Kinetic: Fans (FN)	Pumps (PM)	Motors (MT)	Rotating Machinery (RO)	Other	Non-Facility Event (Explosion) (EX)	Non-Facility Event (Fire) (FT)	Non-Facility Event (Other) (OT)
Working vehicle	-	6	-	-	7	-	-	X	-	X	-	X	-	X	8	X	X	-	-	9	X	-	X	-	X	X	X	X	X	X	-	-	10
Underground refueling operation	-	6	-	-	7	-	-	X	-	X	-	X	-	X	8	X	X	-	-	9	X	-	X	-	X	X	X	X	X	X	-	-	10
Refueling transport vehicle	-	6	-	-	7	-	-	X	-	X	-	X	-	X	8	X	X	-	-	9	X	-	X	-	X	X	X	X	X	X	-	-	10
Fuel transfer (not covered)																																	
Hydrogen mfg. (not covered)																																	

Location (identifier for system, sub-system, or operational feature in this facility section)	Hazard Energy Sources and Materials: Hazard Energy Sources and Materials: Radiological Material (RM)	Fissile Material (FM)	Non-Ionizing Radiation (NI)	Ionizing Rad.: Fissile Material (FM)	Radiography Equipment (RE)	Radioactive Materials (RM)	Radioactive Sources (RS)	Other	Hazardous Materials: Alkali Metals (AM)	Asphyxiants (AS)	Biological (BI)	Carcinogens (CA)	Oxidizers (OX)	Corrosives (CO)	Toxics (TX)	Other	Natural Phenomena: Earthquake (EQ)	Flood (FD)	Lightning (LT)	Rain (RN)	Snow, Ice (SN)	Freezing Weather (FW)	Straight Wind (SW)	Tornado (TO)	Other	Vehicles in Motion: Airplane (AP)	Helicopter (HL)	Train (TN)	Truck/Car (TR)	Forklift/ Lift Truck (FK)	Other	Crane/Hoist (CR)
Working vehicle	-	-	X	-	-	-	X	-	-	11	-	X	X	12	-	13	X	14	15	X	X	X	X	X	16	-	-	X	X	X	17	X
Underground refueling operation	-	-	X	-	-	-	X	-	-	11	-	X	X	12	-	13	X	14	15	-	-	-	-	-	16	-	-	X	X	X	17	X
Refueling transport vehicle	-	-	X	-	-	-	X	-	-	11	-	X	X	12	-	13	X	14	15	X	X	X	X	X	16	-	-	X	X	X	17	X
Fuel transfer (not covered)																																	
Hydrogen mfg. (not covered)																																	

An X refers to the hazards considered applicable.
A number indicated an applicable hazard with an explanation at the end of this Appendix.

Notes

1. High Voltage (HV)

   Voltages above 1000 volts are typically not permitted in the underground environment. (There are exceptions for transmission lines. See the discussion below.) Thus, when the vehicles are underground, there is not exposure to these voltages. If the vehicles exit the mine, there is potential for overhead transmission lines that carry these voltages.

2. Transmission Lines (TL)

   There are instances where 4160 or 7200 volt transmission lines have been installed in mines. These insulated conductors have very limited protection from vehicle impact.

3. Other

   Within the mine there is the potential for exposed conductors, which would be used to support trolley lines. Typically these systems range from 300 to 600 volts DC.

4. Exothermic Reactions (ER)

   The hydrogen-oxygen reaction in the fuelcell is an exothermic reaction

5. Other

   Brake disks on mining equipment can get hot and have been known to cause fires.

6. Pyrophoric (Other)

   The metal hydride is slightly flammable.

   Coal under some conditions can be pyrophoric .

7. Other

   Combustible liquids (flashpoint above 100°F) are present. These can include hydraulic fluids and diesel fuel. The diesel fuel might be contained in transport piping where vehicles are being driven.

   Coal, coal dust and conveyor belts are all present.

8. Other

   Working vehicles might transport explosives.

9. Other

   Pressurized air (~150 psi) and water (-'250 psi) are common.

For vertical shaft or sloped entries there can be considerable potential energy. In addition vehicles can rollover on uneven terrain.

10. Non-Facility Event (Other) (OT)

Surface muting near an underground mine can cause a roof collapse.

11. Asphyxiants (AS)

Black damp has occurred in some mines. This term describes a scenario where an opening is made between an abandoned mine, which is oxygen deficient, and a working none. The oxygen level in the working mine can quickly drop to untenable levels.

Methane is an asphyxiant.

12. Corrosives (CO)

Batteries on the hydrogen-fueled vehicles and nearby vehicles contain acid.

13. Other

There are several materials (e.g., polyurethane) which are used to seal air darns.

Hydrocarbons can leak from walls and the roof of some mines.

14. Flood (FD)

Rapid flooding can occur. Both the rising water and the water flow can cause problems. Water can also collect in low spots where vehicles will need to drive through.

15. Lightning (LT)

Both inside and outside the nine.

16. Other

Roof collapse can range from localized rock falls, which do not damage most vehicles, to extensive collapses.

Bumps are phenomena where the floor will rise or walls will move. It can occur rapidly with no indication. This movement can collapse tunnels crushing the vehicle and its occupants.

17. Other

Other equipment that can be present (e.g., scoops, load haul dumps, roof bolters). Most of these will be characterized as very heavy, difficult to maneuver and with limited operator visibility.

Description of columns in the Hazard Analysis Table

1. *Event Number*

Events are numbered to provide each with a sequential reference.

2. *Event Category*

Events were categorized according to the nature of the postulated release mechanism that directly initiates the postulated consequence. The categories are as follows:

- E-1 Fire
- E-2 Explosion
- E-3 Loss of Containment/Confinement
- E-4 Direct Hazard Exposure
- **E-5** External Hazards
- E-6 Natural Phenomena
- E-7 Other

Events are categorized according to the event description rather than the event initiator. For example, a fire might be a postulated event that causes a tank to burst. This event would fall under category E-2 (Explosion) rather than E-2 (Fire), since the tank rupture is expected to result in a larger consequence than a fire without tank rupture.

3. *Postulated Event Description*

A brief description of a postulated event is given in this column of the Hazard Evaluation Tables. The event description clearly defines the nature of the event. It includes the type of event, its location, hazard source, affected system(s) or equipment, any interaction with other system(s), equipment, and/or hazards, and any pertinent operating characteristics.

4. *Causes*

A cause specifically states the failure, error, operational, and/or environmental condition that initiated. the postulated event. The Hazard Identification Tables were used as a guide in developing specific causes for release events.

5. *Preventive Features*

A preventive feature is any feature that could readily be expected to act to prevent the event from occurring.

6. Frequency Level

Event frequency evaluation is a qualitative or quantitative process that involves assigning a frequency level to each event in the Hazard Evaluation Tables. The hazard analysis team determines which qualitative frequency level is appropriate for a particular event. This determination is based on the event's root cause(s) and may be either qualitative or quantitative. The frequency level is recorded in the Hazard Evaluation Tables according to the definitions in Table 4.

7. Mitigative Features

Mitigative features are any feature that are readily expected to act to reduce the consequences associated with the postulated event. Mitigative features are those which are assumed to be operable during an event or post event, and are not required to be operating prior to the event initiation. Therefore, mitigative features must be capable of withstanding the environment of the event. These might include engineered features (e.g. structures, systems, components, etc.), administrative controls (e.g. procedures, policies, programs, etc.), natural phenomena (e.g. ambient conditions, buoyancy, gravity, etc.), or inherent features (e.g. physical or chemical properties, location, elevation, etc.) operating individually or in combination.

S. Consequences

Event consequences are documented by specifying the potential for loss or damage based on the rankings established in Table 5.

9. Risk *Bin Number*

Using event frequency and consequence levels the hazard analysis team "bins" events in frequency-consequence space to assess relative risk based on Figure 4. The objective of risk binning is to focus attention on those events that pose the greatest risk to the specified receptors. Higher risk events are candidates for additional analysis.

Table 2-1.--Hazard evaluation results

Event		Postulated event	Causes	Preventive features		Freq.	Method of	Mitigative features		Consequence level'		Risk
no.	type	description		design	admin.	level[2]	detection	design	admin.	people	property	bin #
1	E-1	Fire starts remote from vehicle and propagates to involve the hydrogen system. Hydrogen is released.	General fire hazards		Fire protection program	U[3]	Visual, smell	Mine arrangement	Emergency team	H[4]	H	4
2	E-1	Fire starts on vehicle, but not in hydrogen system. Hydrogen is released.	Hot brakes, electrical short	Fuses	Brake maintenance		Visual, smell	Vehicle design, suppression system	Emergency team	H	H	4
3	E-1	Fire starts in hydrogen components. Hydrogen is released	Hydrogen leak		Fire protection program	U	Visual, smell	Hydrogen system integrity	Emergency team	H	H	4
4	E-l	Coal dust ignition by vehicle electrical system. Hydrogen is released	Electrical contacts close	Classified equipment	Inspections	EU	Visual, heat	Mine arrangement	Coal dusting	H	H	7
5	E-2	Battery explosion damages hydrogen system causing leak.	Battery short	Design		U	Visual, equipment fails to run	Design		H	H	
6	E-2	Fire starts remote from vehicle and involves hydrogen system. Hydride tank bursts.	General fire hazards	Relief protection	Fire protection program	EU[5]	Visual, smell	Mine design	Emergency team	H	H	7
7	E-29	Fire starts on vehicle, but not in hydrogen system. Hydride tank bursts.	General fire hazards	Relief protection	Fire protection program	EU	Visual, smell	Vehicle design, suppression system	Emergency team	H	H	7

Table 2-1.--Hazard evaluation results

Event		Postulated event	Causes	Preventive features		Freq.	Method of	Mitigative features		Consequence level'		Risk
no.		description		design	admin.	level[=]	detection	design ,	admin.	people	property	bin #
8	E-2	Fire starts in hydrogen components. Hydride tank bursts.	Hydrogen leak	Relief protection	Fire protection program	EU	Visual, smell	Hydrogen system integrity	Emergency team	H	H	7
9	E-2	Hydrogen explosion	Delayed ignition after leak	Design of vehicle, ventilation		U	Visual	Hydride metal	Emergency team	H	H	7
10	E-2	Methane explosion	Methane release with ignition	Ventilation		A[6]	Meters	Mine layout		H	H	1
I I	E-2	Coal dust explosion	Methane or hydrogen explosion	Ventilation	Coal dusting	EU	Visual, sound	Mine layout		H	H	7
12	E-2	Explosives damage vehicle and release hydrogen	Inadvertent explosion during transport	Packaging		EU	Visual, sound	Hydride metal		H	H	7
13	E-3	Battery leaks acid onto hydrogen system and causes a hydrogen leak.	Battery damage	Design	Vehicle maintenance	EU	Visual		Vehicle inspections	H	H	7
14	E-3	Hydride tanks leak " contents and causes fire	Tank punctured	Design		EU	Visual, smell	Hydride metal selection		H		7
15	E-4	Fuelcell shorts	Damage to membrane	Design		U	Vehicle fails to run			N	L[7]	6
16	E-4	Fuelcell membrane fails and a small deflagration occurs.	Membrane defect	Design		U	Vehicle fails to run			N	L	6
17	E-4	Coal dust enters and damages fuelcell	Filter left off	Design	Training	U	Vehicle fails to run			N	L	6

Table 2-I.--Hazard evaluation results

Event no.	Event type	Postulated event description	Causes	Preventive features: design	Preventive features: admin.	Freq. level[2]	Method of detection	Mitigative features: design	Mitigative features: admin.	Consequence level': people	Consequence level': property	Risk bin # ,
18	**E-4**	Transmission line falls on equipment and damages hydrogen system containment.	Electrical arching		Inspection of transmission lines	EU	Visual	All hydrogen components protected from direct contact	Keep maintenance e access doors on vehicle closed.	H	H	7
19	E-4	Hydrogen system damaged by welding on vehicle	Inattentive welder		Control of welding activities	EU	Visual			*H*	*H*	7
20	**E-4**	Shrapnel damages hydrogen system	Accumulat or ruptures, drive shaft breaks	Design	Vehicle maintenance	EU	Visual, sound	Hydride metal selection		H	11	7
21	**E-4**	Shrapnel damages fuel cell and fire occurs	Accumulat or ruptures, drive shaft breaks	Design	Vehicle maintenance	EU	Visual, sound	Hydride metal selection		H	H	7
22	E-4	Major damage to hydrogen system containment	System dropped during vertical transit			EU	Visual	Hydride metal selection		H	11	7
23	E-4	Vehicle impact damages hydrogen containment	Vehicle to vehicle, vehicle to wall		Training	A	Visual	Vehicle design		H	H	1
24	E-5	Black damp	Open entry to old workings	Shut-off timer	Work planning	U	Visual, low oxygen, high methane content			H	M	4
25	E-5	Acid damage to hydrogen system	Exposure to high acid water	Material selection	Control pH of water	U	Visual		Inspections	H	H	4

Table 2-1.--Hazard evaluation results

Event		Postulated event	Causes	Preventive features		Freq.	Method of	Mitigative features		Consequence level'		Risk
no.	type	description		design	admin.	level[2]	detection	design	admin.	people	property	bin #
26	E-6	Flooding	Water intrusion, pipe break		Work planning	U	Visual	Pumps		H	H	4
27	E-6	Roof collapse[$]		Roof bolting	Inspections	U	Visual	Vehicle design		H	H	4
28	**E 6**	Bump				EU[9]	Visual			H	H	7
29	E-7	Vehicle left in operation after evacuation	Fire, explosion, roof fall causes operator to leave	Shut-off timers		A	Operator interview			L	H	1
30	E-7	Vehicle operated in sub-2% methane	Methane leaks			A				N	L	3

N, negligible; L, low; M, moderate; H, high

[2] A, anticipated; U, unlikely; EU, extremely unlikely; BEU, beyond extremely unlikely.

[3] The frequency that a severe fire would occur in a mine is judged to be unlikely. If it were anticipated, many mines would be experiencing severe fires. This is not the current situation for the mining industry.

["] As discussed in Section 6.4, all events where hydrogen is released have the potential for an explosion. Thus, all events that might lead to a hydrogen release are classified as having a high consequence. This is the bounding consequence for a hydrogen explosion. Those events where ignition of the hydrogen does not occur would be expected to have a lower consequence.

[s] This frequency combines the frequency of a severe fire and the probability that the relief valve fails to operate.

[6] Small-scale explosions resulting from the ignition of small pockets of methane occur in many mines with no significant consequence. Many mines have experienced brief methane flashes at the working face with little or no consequences.

Damage to the membrane is considered to be more than a minor repair.

[$] This event captures all roof collapses. Consequences range from minor damage to equipment that does not require repair, to loss of entire passageway.

[9] The frequency of bumps is judged based on acceptable risk. If bumps are anticipated events, it is judged that the risk of personnel injury would be too high, and the mine would be closed. Thus, they must be unlikely or lower. When combined with the presence of a hydrogen-fueled vehicle the frequency is extremely unlikely.

Appendix B

This example FMEA is for a gaseous hydrogen production method using a steam methane reformer. The excerpt details three components and possible failures associated with those components. This excerpt is typical of most FMEAs, although the complexity of the analysis will vary by project.

Exhibit 2: Excerpt from a Typical Failure Mode and Effects Analysis

Equipment Item	Parameter or Operating Deviation	Cause	Consequences or Implications	Recommendations or Comments
Induced Draft Fan	High reformer draft pressure	Improper function of ID fan suction valve or fan itself	Potential energy release and possible destruction of reformer furnace	Shut down reformer and isolate burner fuel upon reaching a high draft pressure set point
Waste Heat Boilers	High pressure	Line is isolated while boiler is in operation, or pipe scaling occurs due to poor water quality	Pressure relief valves open	A safety relief valve is installed in the piping to release excess gas pressure to the vent stack system. Valves are sized appropriately to accommodate the maximum flow rate at the relieving pressure per the ASME code
	Poor water quality	Improperly functioning deaerator or water treatment system	Accelerated corrosion and scaling occurs in piping and equipment	Periodic testing is performed on the water to determine quality. Not a safety hazard
	Low steam drum level	Poor boiler operation	Low steam-to-carbon ratio could develop in the reformer	Coking could form on the reformer tubes
	Process leaking	External impact or corrosion	Potential for serious burns to personnel	Precautions should be taken to avoid potential impact areas and perform regular quality inspections on the water treatment system
Boiler Feedwater Pumps	Low suction pressure	Low water level in the deaerator	Pump does not prime which results in premature seal wear	On/off pump control will cycle pumps. The reformer will shut down on low steam drum level if the low suction pressure persists

Source: Directed Technologies, Direct-Hydrogen-Fueled Proton-Exchange-Membrane Fuel Cell System for Transportation Applications, Hydrogen Safety Report, DOE/CE/50389-502, 1997. Table 5-1, Hazard Review of On-Site Gaseous Hydrogen Production by Steam Methane Reforming.

Appendix C

Example Risk-binning Matrix

Frequency → / Consequence	Beyond extremely unlikely	Extremely likely	Unlikely	Anticipated
High	**10**	**7**	**4**	**1**
Moderate		**8**	**5**	**2**
Low		**9**	**6**	**3**
Negligible	**11**	**12**		

High risk

Moderate risk

Low risk

Negligible risk

Frequency criteria used for risk-binning

Acronym	**Description**	**Frequency level**
A	Anticipated, Expected	> 1E-2/yr
U	Unlikely	1E – 4 < f ≤ 1E – 2/yr
EU	Extremely Unlikely	1E – 6 < f ≤ 1E – 4/yr
BEU	Beyond Extremely Unlikely	≤ 1E – 6/yr

Consequence criteria used for risk-binning

Consequence level	Impact on populace	Impact on property/operations
High (H)	Prompt fatalities Acute injuries – immediately life threatening Permanent disability	Damage > $50 million Production loss in excess of 1 week
Moderate (M)	Serious injuries Non-permanent disability Hospitalization required	$100,000 < damage ≤ $50 million Vehicle destroyed Critical equipment damaged Production loss less than 1 week
Low (L)	Minor injuries No hospitalization	Damage ≤ $100,000 Repairable damage to vehicle Significant operational down-time Minor impact on surroundings
Negligible (N)	Negligible injuries	Minor repairs to vehicle required Minimal operational down-time No impact on surroundings